

ENTERPRISE DEPLOYMENT OF WINDOWS XP SERVICE PACK 2 WITH ADVANCED SECURITY TECHNOLOGIES

OCTOBER 2004, revised 10/20/2004

With a continued emphasis on providing secure, robust, reliable, and cost-effective solutions to our school districts, administrators, teachers, and students, the Kentucky Department of Education Office of Education Technology is providing these detailed instructions on the deployment of Windows XP Service Pack 2 throughout the KETS environment.

TABLE OF CONTENTS

- I. BACKGROUND INFORMATION
- II. CHANGES IN WINDOWS XP SERVICE PACK 2 WITH
ADVANCED SECURITY TECHNOLOGIES
- III. DEPLOYMENT METHODOLOGY

I. BACKGROUND INFORMATION

Late in 2001 Microsoft Corporation released the Windows XP desktop operating system with great fanfare. It offered several enhancements over previous operating systems. In the fall of 2002 they released the first service pack for this product that included a wide variety of security fixes as part of Microsoft's Trustworthy Computing initiative along with enhancements for newer technologies like Universal Serial Bus (USB) 2.0.

In February 2004, districts were provided documentation for the installation of a Microsoft Software Update Services server. The purpose of this server is to provide Critical hotfixes and patches to Microsoft Windows 2000, Windows XP, and Windows 2003 workstations and servers.

In August 2004, service pack 2 for Windows XP was released to the public. The Kentucky Department of Education Office of Education Technology had been testing this service pack for several months prior to its release and realized that certain portions of this product could create technical hurdles for the school districts across our state. We proactively issued a statement to districts stating that we were placing a block on all district domains to prevent the "typical" enduser from downloading the service pack via Automatic Updates. This block did not stop district technology administrators from manually downloading the service pack for testing purposes. We informed district technology administrators both via their respective KETS Engineers and security webcasts that they should refrain from deploying Windows XP Service Pack 2 until further testing and deployment strategies could be devised.

In early October 2004, the Kentucky Department of Education Technology Office of Education Technology implemented a policy on each district domain that turns off the firewalling feature of the service pack until such time that a full understanding of its benefits and pitfalls have been gained.

II. CHANGES IN WINDOWS XP SERVICE PACK 2 WITH ADVANCED SECURITY TECHNOLOGIES

There are several significant changes that follow the installation of Windows XP Service Pack 2 including a firewall, popup blocking, enhanced privacy protection, and much improved wireless network handling. A list of features included in Windows XP Service Pack 2 can be found at <http://www.microsoft.com/windowsxp/sp2/features.mspx>.

A list of the Top Ten Reasons to Install found at <http://www.microsoft.com/windowsxp/sp2/topten.mspx> are shown below:

Top 10 Reasons to Install Windows XP Service Pack 2 (SP2)

- 1 Help protect your PC from harmful attachments.**
By alerting you to potentially unsafe attachments, [Windows XP Service Pack 2](#) (SP2) helps guard your computer from viruses that can spread through Internet Explorer, Outlook Express, and Windows Messenger.
- 2 Improve your privacy when you're on the Web.**
SP2 helps protect your private information by applying the security settings that guard your PC to the files and content downloaded using Internet Explorer.
- 3 Avoid potentially unsafe downloads.**
Internet Explorer download monitoring and the [Internet Explorer Information Bar](#) warn you about potentially harmful downloads and give you the option to block files that could be malicious.
- 4 Reduce annoying pop-ups.**
[Internet Explorer Pop-Up Blocker](#) makes browsing the Internet more enjoyable by helping you reduce the unwanted ads and content that pop up when you're browsing the Web.
- 5 Get firewall protection from startup to shutdown.**
The powerful, built-in [Windows Firewall](#) is now turned on by default. This helps protect Windows XP against viruses and worms that can spread over the Internet.
- 6 Take control of your security settings.**
The new [Windows Security Center](#) allows you to easily view your security status and manage key security settings in one convenient place.



Get the latest updates easily.

Enhancements to Windows XP's Automatic Updates feature make it even easier to access Windows updates. Plus, new technology has been added to help dial-up customers download updates more efficiently.



Help protect your e-mail address.

[Improvements to Outlook Express](#) help reduce unwanted e-mail by limiting the possibility of your e-mail address being validated by potential spammers.



Take action against crashes caused by browser add-ons.

The new Add-On Manager in Internet Explorer lets you easily view and control add-ons to reduce the potential for crashes and enjoy a more trouble-free browsing experience.



Go wireless without the hassle.

SP2 improves wireless support and simplifies the process of discovering and connecting to wireless networks in your home or on the road.

III. DEPLOYMENT METHODOLOGY

PLEASE NOTE THAT DUE TO THE SIZE OF WINDOWS XP SERVICE PACK 2, THE DISTRICT MICROSOFT SOFTWARE UPDATE SERVICES SERVER (SUS) WILL NOT BE USED TO UPDATE THE BULK OF THE WORKSTATIONS. ONCE ALL DISTRICTS HAVE COMPLETED THEIR INSTALLATION OF SERVICE PACK 2, THE SUS VERSION WILL BE APPROVED FOR DISTRIBUTION ON ANY ADDITIONAL WORKSTATIONS.

A thorough review of deployment options has been performed and the list below provides the recommendations that best fit the KETS environment based upon individual district LAN/WAN topology:

1. ALL FIBER CONNECTED DISTRICT

- i. A centralized network share and a group policy should be created to deploy the service pack.

1. Steps for implementation

- a. Create a share on a file server at a central location and name it XPSP2.
 - b. Remove the Everyone group permissions to the share.
 - c. **Give the <District Domain>\DIST Support Admins Full Control permissions to the share.**
 - d. **Give the ketsds.net\Enterprise Admins group Read Permissions to the share.**
 - e. Give the Domain Computers group Read permissions to the share.
 - f. Copy the file <ftp://ketsftp.k12.ky.us/WinXP/XPSP2.zip> and extract it into the share folder. **Please note that this file is nearly 300MB and should be downloaded after normal business hours.**
 - g. Email your KETS Engineer and inform him that you need the “ALL FIBER” Group Policy Object Created and linked to your “Workstations” OU. You will need to include the NETBIOS name and IP address

of the file server upon which you created the share.

- h. Your KETS Engineer will contact the KETS Help Desk and open a ticket for this policy creation.
- i. The Enterprise Directory Services Team will create the group policy and will link it to the “Workstations” OU on the Friday afternoon following completion of the request. The KETS Engineer and the district technology staff will be notified that the policy has been created and is awaiting deployment.
- j. The district technology staff will need to issue a statement to their endusers to reboot their workstations before leaving for the weekend on that Friday.

2. ALL OTHER DISTRICTS

- i. Network file shares should be created at each location at the end of a WAN link.

- 1. Steps for implementation

- a. Create a share on each file server at the school locations and name each XPSP2.
 - b. Remove the Everyone group permissions to the shares.
 - c. **Give the <District Domain>\DIST Support Admins Full Control permissions to the share.**
 - d. **Give the ketsds.net\Enterprise Admins group Read Permissions to the share.**
 - e. Give the Domain Computers group Read permissions to the shares.
 - f. Copy the file <ftp://ketsftp.k12.ky.us/WinXP/XPSP2.zip> and extract it into each shared folder.
Please note that this file is nearly 300MB and should be downloaded after normal business hours.
 - g. Email your KETS Engineer and inform him that you need the “INDIVIDUAL

SCHOOL” Group Policy Object Created and linked to your respective “Workstations/<SCHOOL NAME>” OUs.

You will need to include the NETBIOS name and IP address for each of the file servers upon which you created the share.

- h. Your KETS Engineer will contact the KETS Help Desk and open tickets for the creation of these policies.
- i. The Enterprise Directory Services Team will create the group policies and will link them to the respective “Workstations/<SCHOOL NAME>” OU on the Friday afternoon following completion of the request. The KETS Engineer and the district technology staff will be notified that the policy has been created and is awaiting deployment.
- j. The district technology staff will need to issue a statement to their endusers to reboot their workstations before leaving for the weekend on that Friday.

PLEASE NOTE THAT IF A DISTRICT WANTS TO DEPLOY ONLY ONE LOCATION AT A TIME, EXCEPTIONS WILL BE ACCOMODATED.

Any questions/concerns should be sent to helpdesk@kde.state.ky.us for clarification. They can also be reached at 866-KETS-HELP.